CVD-Richtlinie

Stand: August 2026

1. Zweck

Die Pütz Group legt großen Wert auf die Sicherheit ihrer Produkte, Systeme und Dienstleistungen. Diese Coordinated Vulnerability Disclosure Policy beschreibt den Prozess zum Umgang mit Sicherheitslücken bei den Firmen der Pütz Group. Es soll allen Anwendern unserer Produkte und Lösungen alle Informationen bereitstellen, die sie benötigen, um auf etwaige Cybersicherheitsprobleme oder Sicherheitslücken, die in unseren Produkten entdeckt werden, vorbereitet zu sein.

Unser Ziel ist es, gemeldete Schwachstellen gemeinsam mit den Meldenden zu analysieren, Risiken zu bewerten und geeignete Maßnahmen zur Behebung oder Risikominderung zu entwickeln, bevor sicherheitsrelevante Informationen veröffentlicht werden.

2. Gesetzliche Vorgaben

Dieser Prozess zum Umgang mit Sicherheitslücken erfüllt die Verpflichtungen gemäß dem EU-CRA Cyber Resilience Act.

3. Geltungsbereich

Diese Policy gilt für Produkte, Software und Dienstleistungen der Pütz Group, insbesondere:

- Softwareprodukte der Pütz Group
- Industrie-PCs, Embedded-Systeme und Edge-Geräte
- Lösungen zur Prozessautomatisierung
- Visualisierungssysteme (HMI)
- SCADA- und Leitsystemkomponenten
- Kommunikationslösungen und Gateways
- Remote-Service- und Fernwartungslösungen
- Cloud-Dienste und Webanwendungen der Pütz Group
- Mobile Anwendungen der Pütz Group

Nicht vom Geltungsbereich umfasst sind:

- Produkte anderer Hersteller
- Kundenspezifische Netzwerke oder Anlagenkonfigurationen
- Systeme, die durch Kunden oder Integratoren verändert wurden und deren Verhalten nicht mehr dem Auslieferungszustand entspricht

4. Meldung einer Sicherheitslücke

Sicherheitslücken können jederzeit gemeldet werden an: **E-Mail: security@puetzgroup.de**

Bitte stellen Sie möglichst folgende Informationen zur Verfügung:

- Name des betroffenen Produkts
- Software- bzw. Firmware-Version
- Beschreibung der Schwachstelle
- Voraussetzungen für die Ausnutzung
- Schrittweise Reproduktionsanleitung
- Machbarkeitsnachweis (Proof of Concept) falls vorhanden
- Einschätzung der möglichen Auswirkungen
- Kontaktdaten für Rückfragen

Falls vertrauliche Informationen übermittelt werden, empfehlen wir eine verschlüsselte Kommunikation.

5. Bearbeitung von Meldungen

Nach Eingang einer Meldung erfolgt der folgende Bearbeitungsprozess:

Schritt:	**Ziel:**
Eingangsbestätigung	innerhalb von 5 Arbeitstagen
Erste technische Bewertung	innerhalb von 10 Arbeitstagen
Rückmeldung zum weiteren Vorgehen	sobald die Bewertung abgeschlossen ist
Entwicklung von Gegenmaßnahmen	abhängig von Kritikalität und Komplexität
Veröffentlichung eines Security Advisory	nach Bereitstellung geeigneter Gegenmaßnahmen oder Mitigationsmaßnahmen

Bei besonders komplexen Sachverhalten oder wenn Drittanbieter beteiligt sind, können längere Bearbeitungszeiten erforderlich sein. In diesem Fall informieren wir den Meldenden regelmäßig über den Bearbeitungsstand.

6. Koordinierte Offenlegung (Coordinated Vulnerability Disclosure)

Die Pütz Group verfolgt den Grundsatz der koordinierten Offenlegung von Sicherheitslücken.

Dies bedeutet:

- Die gemeldete Schwachstelle wird zunächst vertraulich behandelt.
- Der Meldende erhält eine Rückmeldung über den Bearbeitungsstand.
- Eine öffentliche Veröffentlichung erfolgt erst, nachdem geeignete Gegenmaßnahmen verfügbar sind oder das verbleibende Risiko angemessen bewertet wurde.
- Veröffentlichungszeitpunkt und Inhalt werden – soweit möglich – mit dem Meldenden abgestimmt.

7. Safe Harbor

Die Pütz Group unterstützt verantwortungsvolle Sicherheitsforschung.
Wir werden keine rechtlichen Schritte gegen Personen einleiten, die:

- in gutem Glauben handeln
- ausschließlich der Identifizierung und verantwortungsvollen Meldung von Sicherheitslücken dienen
- keine Daten verändern, löschen oder veröffentlichen
- keine personenbezogenen Daten oder Betriebsgeheimnisse missbräuchlich verwenden
- die Verfügbarkeit unserer Systeme nicht beeinträchtigen
- keine Social-Engineering-Angriffe durchführen
- keine Denial-of-Service-Angriffe durchführen
- keine Schadsoftware einsetzen
- nach Entdeckung einer Schwachstelle ihre Aktivitäten unverzüglich einstellen und uns informieren

Diese Zusicherung gilt ausschließlich für Handlungen im Rahmen dieser Policy und im gesetzlich zulässigen Umfang.

8. Umgang mit CVEs

Sofern eine gemeldete Schwachstelle die Vergabe einer Common Vulnerabilities and Exposures (CVE)-Kennung rechtfertigt, wird die Pütz Group:

- die Vergabe einer CVE koordinieren oder unterstützen
- mit zuständigen CVE Numbering Authorities (CNA) zusammenarbeiten
- die CVE-Nummer in ihren Security Advisories veröffentlichen
- betroffene Produkte eindeutig benennen

9. Security Advisories

Für bestätigte sicherheitsrelevante Schwachstellen veröffentlicht die Pütz Group bei Bedarf Security Advisories.

Diese enthalten insbesondere:

- Beschreibung der Schwachstelle
- betroffene Produkte und Versionen
- Schweregrad (z. B. CVSS)
- mögliche Auswirkungen
- verfügbare Sicherheitsupdates
- empfohlene Mitigationsmaßnahmen
- Referenzen zu CVE-Nummern (falls vorhanden)

10. Besonderheiten industrieller Systeme

Die Produkte der Pütz Group werden in industriellen Umgebungen eingesetzt, in denen Anlagenverfügbarkeit und funktionale Sicherheit höchste Priorität besitzen. Daher können Sicherheitsupdates nicht immer unmittelbar bereitgestellt oder installiert werden. In solchen Fällen veröffentlichen wir geeignete Mitigationsmaßnahmen, um Risiken bis zur Bereitstellung eines Updates zu reduzieren.

Vor der Freigabe von Sicherheitsupdates werden diese sorgfältig hinsichtlich Funktionalität, Stabilität und Kompatibilität geprüft.

11. Vertraulichkeit

Alle eingehenden Meldungen werden vertraulich behandelt.

Personenbezogene Daten werden ausschließlich zur Bearbeitung der Meldung verwendet und entsprechend den geltenden Datenschutzbestimmungen verarbeitet.

Der Name des Meldenden wird nur mit dessen ausdrücklicher Zustimmung veröffentlicht.

12. Anerkennung

Die Pütz Group bedankt sich bei allen Personen, die durch verantwortungsvolle Meldungen zur Verbesserung der Sicherheit unserer Produkte beitragen.

Eine finanzielle Vergütung (Bug Bounty) wird derzeit nicht angeboten.

13. Änderungen

Diese Coordinated Vulnerability Disclosure Policy wird regelmäßig überprüft und bei Bedarf an neue regulatorische oder technische Anforderungen angepasst.